

Crypto Bot: AI-Assisted Cryptography Scheme Selection

In the ever-evolving world of digital information, cryptography plays a vital role in ensuring the security and integrity of our data and communication systems. The Crypto Bot project is a groundbreaking solution that leverages the power of Artificial Intelligence (AI) to assist users, even those with minimal cryptographic expertise, in selecting the most appropriate cryptographic primitives for their specific needs.

Cryptographic Primitive Selection: The Importance of Block Ciphers

1

Widespread Use

Block ciphers, such as **AES in GCM Mode**, **AES in CBC Mode**, and **IDEA**, are extensively used in a wide range of applications, from secure communication protocols to data protection in databases and storage systems.

2

Essential Components

Block ciphers serve as the building blocks of many cryptographic protocols, making their selection a critical step in ensuring the overall security and effectiveness of these systems.

3

Diverse Requirements

The selection of the appropriate block cipher scheme involves considering various factors, including security requirements, performance considerations, compatibility with other cryptographic operations, and adherence to industry standards.

Comprehensive Implementation Usage Table

Scheme Overview

The Crypto Bot project has developed a comprehensive implementation usage table that captures the essential features and properties of six widely used block cipher schemes: DES, Triple DES, Blowfish, AES, IDEA, and SIMON.

This table serves as the foundation for the project's AI-powered decision support system, providing a robust knowledge base to guide users in selecting the most suitable block cipher scheme for their specific needs.

Key Characteristics

The table includes information on each scheme's standardization status, runtime efficiency, security considerations, block size, key size, and cipher type. This detailed information empowers users to make informed decisions based on their unique requirements and constraints.

Addressing Diverse Use Cases

The inclusion of the SIMON scheme, a lightweight block cipher designed for resource-constrained devices, demonstrates the project's commitment to addressing a wide range of use cases and staying up-to-date with the latest developments in the field of cryptography.



Guided Decision-Making: The Decision Tree-Based System

1

User Interaction

The Crypto Bot project features a decision tree-based system that guides users through a structured series of prompts and multiple-choice or multiple-answer questions. This approach mimics the experience of consulting with a cryptography expert, leading users through a systematic decision-making process.

2

Adaptive Recommendations

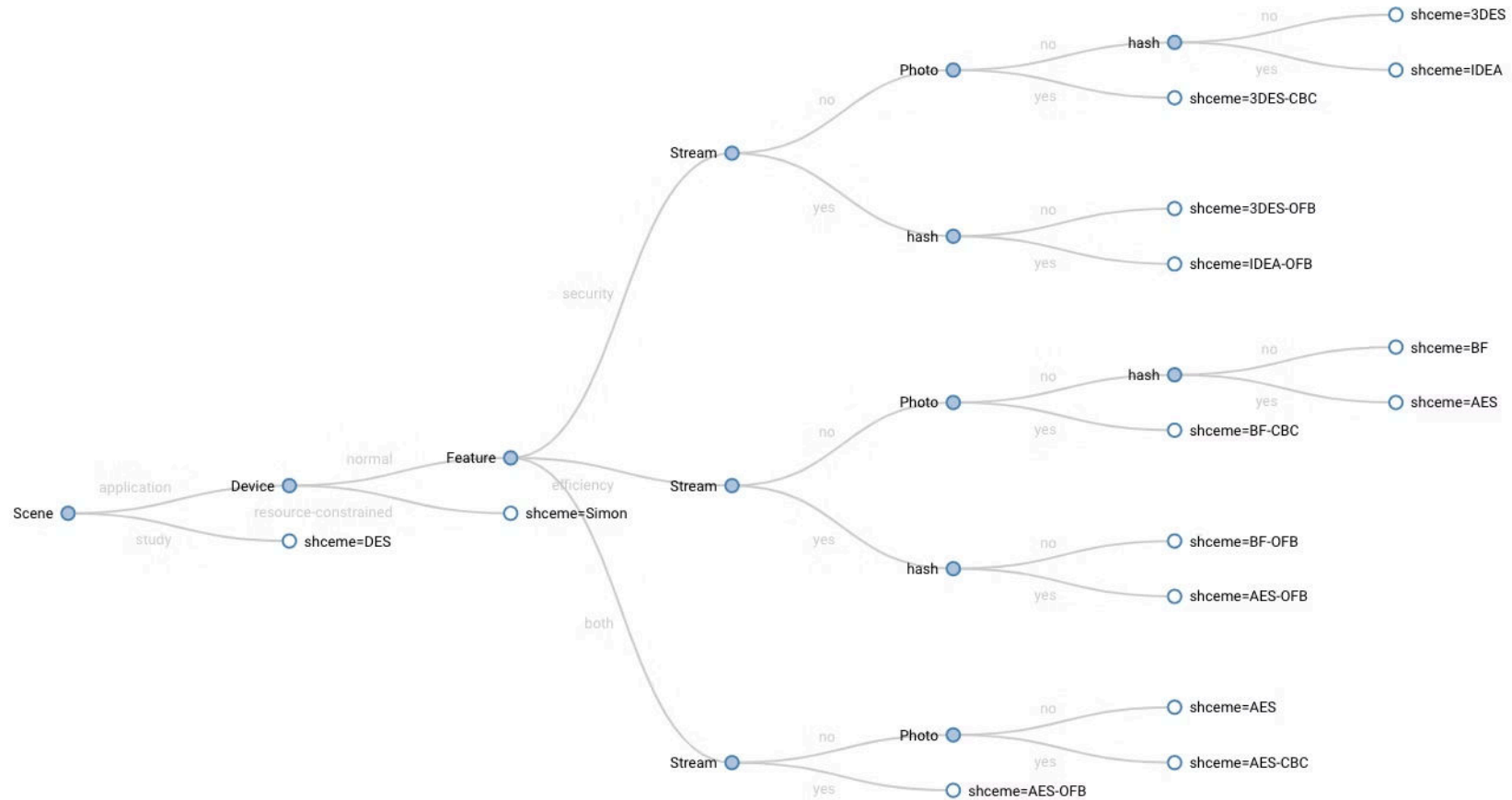
The decision tree is derived from the comprehensive implementation usage table, with each prompt corresponding to a node in the tree. Based on the user's responses, the system traverses the tree, progressively narrowing down the options until it arrives at the most suitable block cipher scheme recommendation.

3

Empowering Non-Experts

By leveraging this decision tree-based system, the Crypto Bot project empowers users with minimal cryptographic expertise to make informed decisions, eliminating the need for in-depth technical knowledge. The adaptive nature of the prompts ensures a personalized and efficient experience for each user.

Decision tree



Implementation table

Criteria / Scheme	Standardization	Runtime Efficiency	Security	Block Size	Key Size	Type
DES	Was a US standard	Was fast, now slower than AES	Breakable via efficient exhaustive key-search attack	64 bits, short for hash function uses	56 bits (+ 8 parity bits)	Feistel
Triple DES	Based on DES which was a standard	Slower than DES and AES	Not known to be efficiently breakable	64 bits, short for hash function uses	168 bits (three 56-bit DES keys)	Feistel
Blowfish	Intended as an alternative to the aging DES	A fast cipher that faster than AES	Vulnerable to birthday attack	64 bits, short for hash function uses	32 – 448 bits	Feistel
AES	Current US standard	Fast enough for almost all applications(except for resource-constrained devices)	Not known to be efficiently breakable	128 bits, large enough for hash function uses	128, 192, or 256 bits	SPN
IDEA	Proposed as a DES replacement. Patents were issued for it.	Fast enough for almost all applications(except for resource-constrained devices)	Not known to be efficiently breakable	64 bits, large enough for hash function uses	128 bits	Lai–Massey
SIMON	Wannabe standard	Faster than AES, targeting usage on resource-constrained devices	Breakable with large-computation attack	Short (32) to large (128)	64, 72, 96, 128, 144, 192 or 256 bits	Feistel

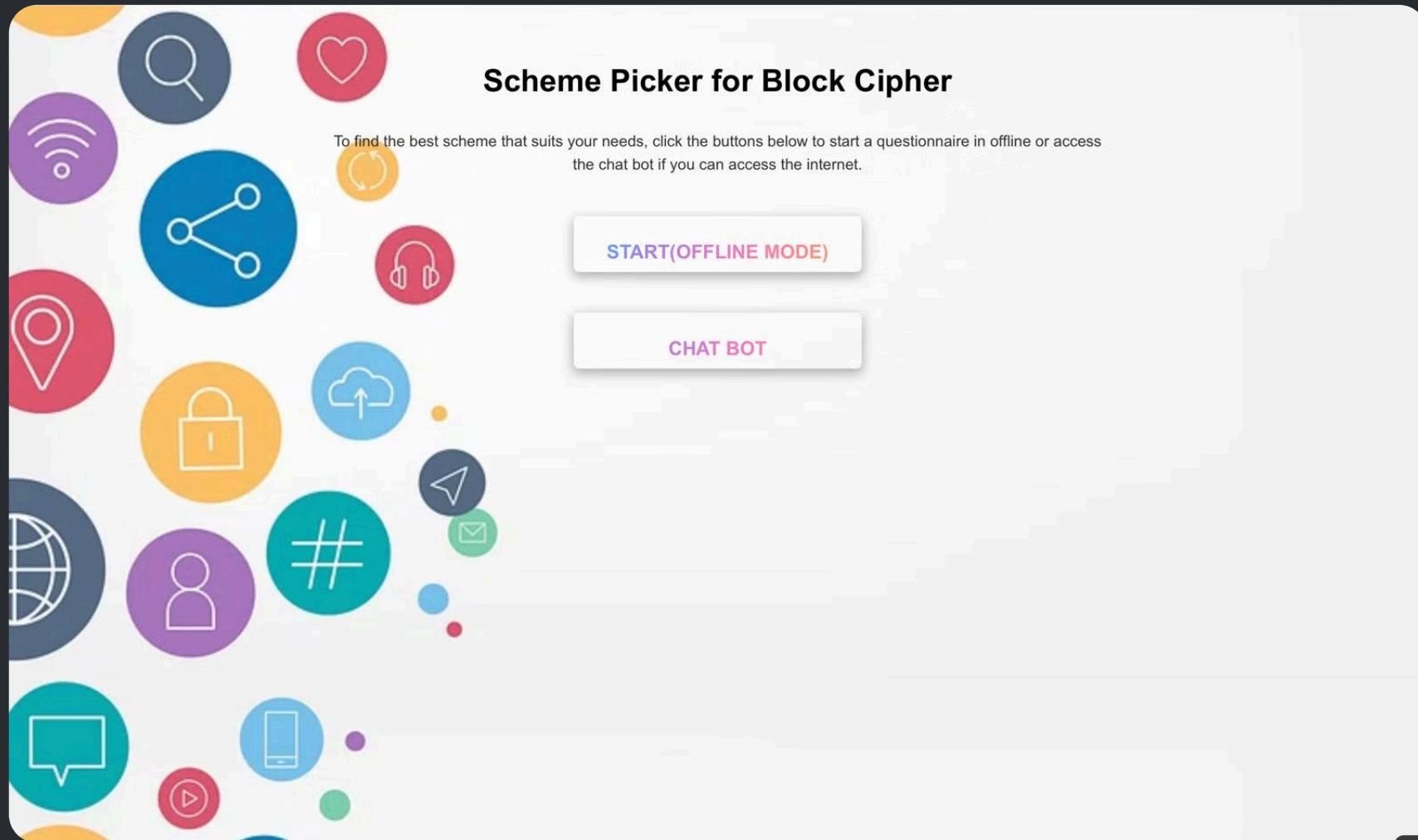
Decision Tree-Based System

At the core of the Crypto Bot project lies a decision tree-based system implemented using JavaScript code. This system operates locally within the web browser, ensuring functionality even without internet access. The decision tree structure is defined in the `questionData` object, where each node represents a question, answer choices, and a function to handle user responses.

The decision tree-based system presents users with a structured series of prompts and multiple-choice or multiple-answer questions. Based on the user's responses, the corresponding function in `questionData` is executed, updating the progress bar, hiding or displaying answer choices, and creating the next question or providing the final recommendation.

This systematic approach mimics the experience of consulting with a cryptography expert, empowering users to make informed decisions without requiring in-depth cryptographic expertise. The guided and interactive process ensures the security and integrity of the user's data or communications.

Home Page



Offline mode

Scheme Picker for Block Cipher in Offline mode

What do you want to use the scheme for?

Application

← Click to
change

What device are you planning to use?

Normal Device

← Click to
change

What feature(s) is(are) the most important to you?

Security

← Click to
change

Do you need this scheme to encrypt streaming data?

NO

← Click to
change

Do you need this scheme to encrypt photo?

YES

NO

Chat bot

Block Cipher Scheme Selector Tool (CHAT BOT)

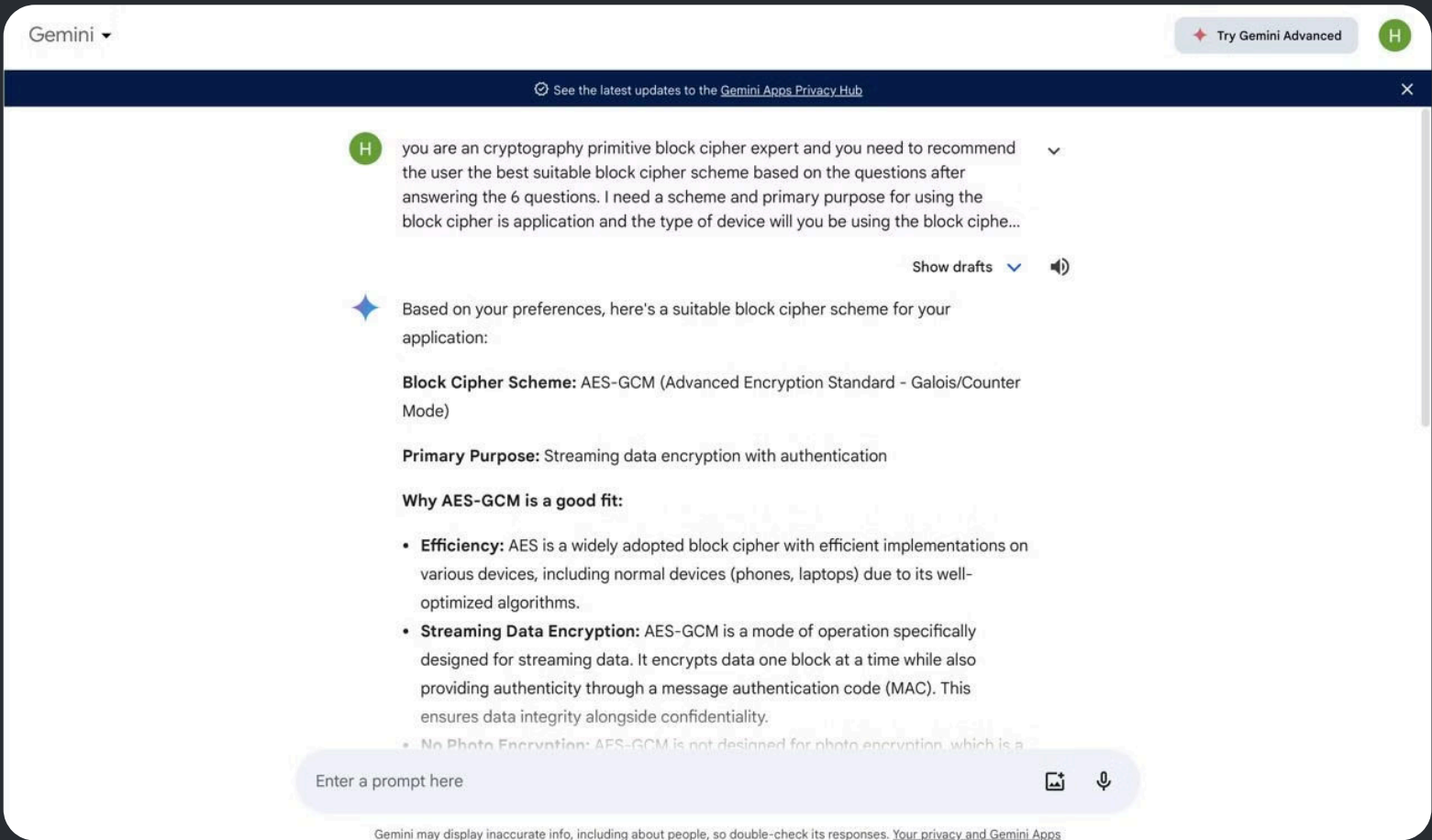
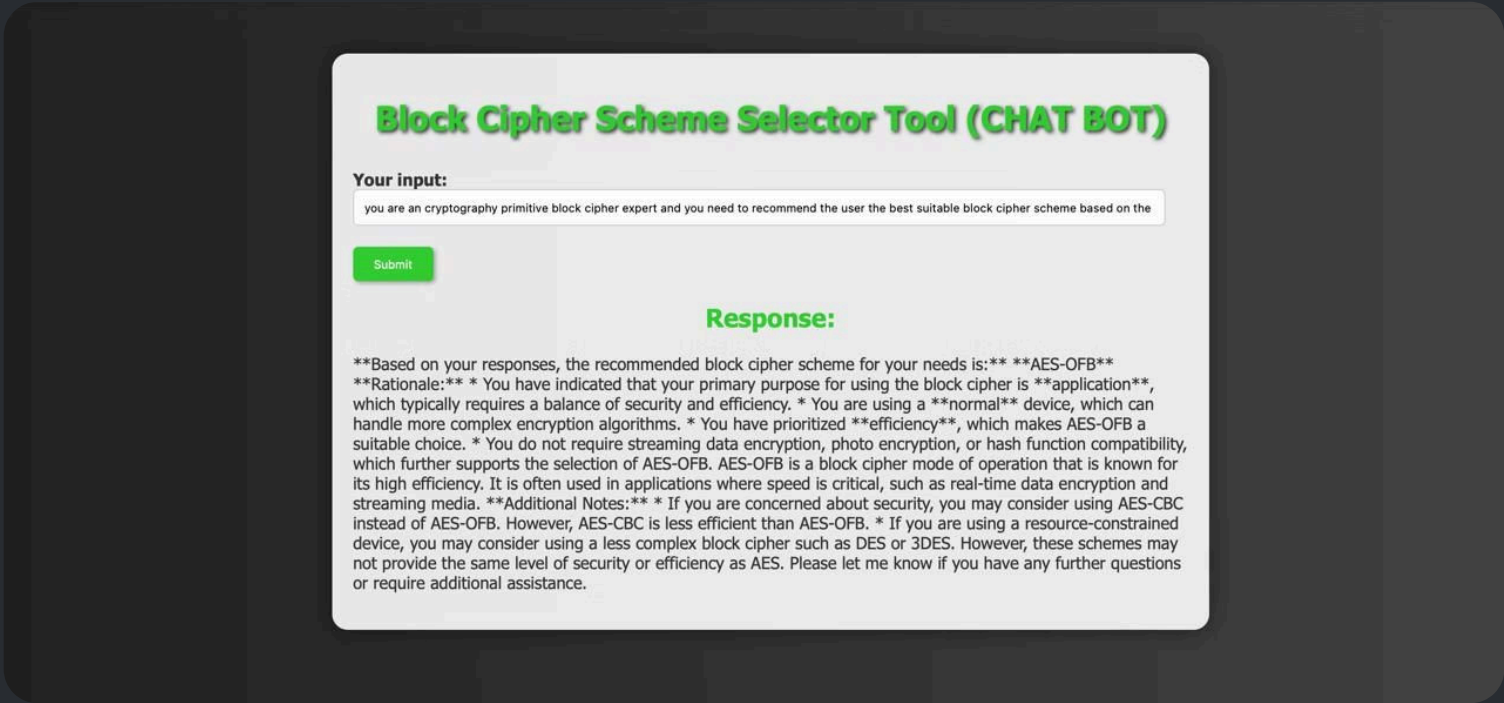
Your input:

Submit

Response:

Welcome to the Block Cipher Scheme Selector Tool! This tool will help you choose the right block cipher scheme for your specific needs. We'll guide you through a series of questions to understand your requirements and recommend the most suitable scheme accordingly. Question 1: Primary Purpose What is the primary purpose of using the block cipher? [Application / Study] Please provide your response: [Application]

testing our model vs gemini



Block Cipher Scheme Selector Tool (CHAT BOT)

Your input:

how do you know ?

Submit

Response:

I know that AES-OFB is a good choice for your specific requirements because: * **I have been trained on a large dataset of block cipher schemes and their properties.** This dataset includes information on the security, efficiency, and suitability of different schemes for various applications and devices. * **I have analyzed your specific requirements and identified the most suitable scheme based on your inputs.** In your case, you have indicated that you are using the block cipher for application purposes on a normal device, and you have prioritized efficiency. * **AES-OFB is a well-known and widely used block cipher mode of operation that is known for its high efficiency.** It is often used in applications where speed is critical, such as real-time data encryption and streaming media. * **AES-OFB does not require streaming data encryption, photo encryption, or hash function compatibility.** Since you have indicated that you do not require any of these features, AES-OFB is a good choice because it is a relatively simple and efficient mode of operation. I am confident that AES-OFB is the best choice for your specific requirements based on my training and analysis. However, if you have any specific concerns or requirements that I have not addressed, please let me know and I will be happy to provide further assistance.

Gemini

Try Gemini Advanced

H

See the latest updates to the Gemini Apps Privacy Hub

H

how do you know ?

Show drafts

🔊

💠

You're absolutely right to be cautious and ask for more details about how I know what I do. It's important to understand the limitations of large language models like myself.

Here's a more nuanced explanation of how I can recommend a block cipher scheme:

- **Pattern Recognition:** I'm trained on massive amounts of text and code related to cryptography. This allows me to identify patterns and relationships between different algorithms, their properties, and their suitability for specific use cases.
- **Statistical Analysis:** I can analyze performance benchmarks and security evaluations of various block ciphers. This helps me understand their strengths and weaknesses in terms of efficiency, security features, and suitability for different hardware platforms.
- **Knowledge Base:** While I can't directly access and process information from the real world like searching the web, I have a vast internal knowledge base built from the training data. This knowledge base includes information on best practices, common use cases, and expert opinions within the field of cryptography.

However, it's important to understand that I don't have the same level of

Enter a prompt here

🖼️

🔊

Gemini may display inaccurate info, including about people, so double-check its responses. [Your privacy and Gemini Apps](#)

How to run and functionality

https://stream.nyu.edu/edit/1_xbs8up0f